• F I N A N S E I P R A W O F I N A N S O W E •
• Journal of Finance and Financial Law •

Czerwiec/June 2018 • vol. 2(18): 65–78

https://doi.org/10.18778/2391-6478.2.18.06

NOWE ZAGROŻENIA A METODY OCHRONY USŁUG FINANSOWYCH W SEKTORZE BANKOWOŚCI MOBILNEJ NA PRZYKŁADZIE STUDENTÓW LUBELSKICH UCZELNI

Magdalena Sobiesiak, Paweł Zagrodniczek
Wydział Ekonomiczny
Uniwersytet Marii Curie-Skłodowskiej w Lublinie

Streszczenie

Celem niniejszego artykułu jest zbadanie świadomości konsumentów w zakresie korzystania z bankowości mobilnej w Polsce. Zaprezentowano również ewolucję bankowości mobilnej, a także skalę zjawiska jej występowania. Opracowanie przedstawia wyniki badania kwestionariuszowego przeprowadzonego wśród studentów lubelskich uczelni dotyczącego poziomu wiedzy oraz typowych nawyków podczas korzystania z m-bankingu. Ponadto w oparciu o informacje prezentowane przez wybrane banki i instytucje sektora finansowego zostały omówione przykładowe metody działania cyberprzestępców.

Słowa kluczowe: bankowość mobilna, bankowość wirtualna, technologie mobilne, cyberprzestępczość.

JEL Class: G20, G21, G29.

WPROWADZENIE

W czasach stale rosnącej konkurencji systemu bankowego w Polsce, ogromną rolę odgrywa bankowość elektroniczna. Banki udostępniają szeroki wachlarz usług, wprowadzając bankowość elektroniczną, która obsługiwana za pomocą między innymi Internetu umożliwia klientom banków dostęp do rachunku bankowego i czynności z nim związanych w szerszym otoczeniu niż placówka banku. Przyczyniło się to do udogodnienia korzystania z usług bankowych. Bankowość elektroniczna to dostęp do usług oferowanych przez banki w celu zarządzania swoim rachunkiem, za pośrednictwem komputerów, bankomatów czy telefonów stacjonarnych. Ważną rolę w poszerzaniu zakresu oddziaływania przez banki w bankowości elektronicznej odgrywa jej młodsza siostra – bankowość mobilna – która dostosowując się do obecnych trendów i wymagań konsumentów – oparta jest na urządzeniach bezprzewodowych, które ponadto umożliwiają korzystanie z aplikacji w celu zarządzania swoim rachunkiem bankowym. Jest to konsekwencją rozwoju cywilizacyjnego, który niesie za sobą szereg zmian i zwiększa potrzeby konsumentów, jak również poszerza oczekiwania w stosunku do banków. Wymagania stawiane bankom, które aby utrzymać swoją pozycję na rynku próbują im sprostać, uskuteczniły rozwój bankowości, poprzez zdalne systemy bankowości [Guzek i Ślązak 2012: 19]. Mobilność w czasach obecnych jest nieodłącznym elementem bytowania człowieka, ponieważ ludzie cenią sobie wygodę i czas. Zauważalne jest zjawisko ograniczenia wykorzystywania druków, potwierdzeń czy papierowych wyciągów, duża grupa odbiorców preferuje mieć wszystko łatwo dostępne, pod ręką, aby w każdej chwili można było kontrolować swoje wydatki lub ograniczyć przechowywanie kapitału w gotówce. Bankowość mobilna mimo wielu zalet ma jednak również wady, o których nie można zapomnieć. Za cel artykułu postawiono weryfikację hipotezy, że obecny poziom wiedzy uniemożliwia w pełni bezpieczne korzystanie z innowacyjnych rozwiązań, jakie oferuje bankowość mobilna.

1.1. POJĘCIE BANKOWOŚCI MOBILNEJ – HISTORIA BANKOWOŚCI W POLSCE

Bankowość mobilna oznacza korzystanie z rachunku bankowego za pomocą telefonów komórkowych, smartfonów czy tabletów. Za pomocą wspomnianych urządzeń posiadacze rachunków bankowych mogą mieć swobodny dostęp do nich. Umożliwia im to np. sprawdzanie stanu konta, wykonywanie operacji finansowych, czy wydawanie dyspozycji dotyczących posiadanej przez nich karty. Ogromną zaletą bankowości mobilnej jest fakt, iż przy wykorzystaniu Internetu bądź aplikacji bankowych off-line mają do niego dostęp w każdej chwili.

Patrząc na bankowość mobilną z historycznego punktu widzenia, można stwierdzić, że w przypadku Polski nie odbiega ona znacząco w czasie względem powstania bankowości internetowej. Początki bankowości mobilnej w Polsce sięgają 1999 roku, kiedy miało miejsce wprowadzenie przez Wielkopolski Bank Kredytowy powiadomień SMS o operacjach na rachunku posiadacza. Jedynym warunkiem był fakt posiadania przez klienta telefonu w sieci GSM PLUS. Pozwalało to na kontrolowanie rachunku bankowego za pomocą telefonu komórkowego. Dostępne usługi opierały się na możliwości nie tylko sprawdzenia salda, ale też pięciu transakcji ostatnio wykonanych. Kolejnym kanałem były protokoły WAP [Pearce 2013: 28–29] wprowadzone przez ten sam bank w 2000 r. Cechowała je innowacyjność, ze względu na fakt, iż dzięki nim użytkownik mógł wykorzystywać dostępną mu przeglądarkę do dokonywania podstawowych operacji finansowych. Następnym krokiem było wprowadzenie na rynek w 2004 roku pierwszej mobilnej aplikacji SIM Toolkit – „Płacę SMSem" w systemie Inteligo. Natomiast w 2009 roku w systemie iOS – Raiffeisen Bank Polska, wykorzystał aplikacje mobilne oddając je do użytku swoim klientom. Rok później możliwość tę wprowadził Alior Bank, a dwa lata później Bank Millenium, Bank Zachodni WBK, Citi Handlowy, Bank Pekao i mBank. Z każdym rokiem coraz więcej banków wbogacało formy obsługi klienta o bankowość mobilną. Rozwijała się również jej funkcjonalność i oddziaływanie na klienta. Pod koniec 2012 roku z aplikacji mobilnych korzystało 1,2 milionów klientów banków. Z kolei 2013 rok był czasem przemian i debiutów. Po pierwsze wyszła pierwsza aplikacja mobilna na tablety wprowadzona przez ING Bank Śląski, zadebiutowały płatności PeoPay, a także system płatności mobilnych IKO. Dodatkowo banki powołały Polski Standard Płatności, a w sklepach rozpoczęto wprowadzanie mobilnych płatności. Pod koniec 2015 roku aż 5 milionów klientów banków korzystało z bankowości mobilnej.

1.2. OBECNA SYTUACJA BANKOWOŚCI MOBILNEJ W POLSCE

Wprowadzenie bankowości mobilnej rozpoczęło rewolucję w dostarczaniu usług oferowanych przez banki [Niczyporuk i Talecka 2011: 203–204] oraz otworzyło nowe okno na świat. Polacy chętnie korzystają z tego typu udogodnień. Rosnąca liczba smartfonów wpływa znacząco na rozszerzanie się oddziaływania aplikacji mobilnych. Z końcem IV kwartału 2017 roku liczba użytkowników bankowości mobilnej wynosiła 8,9 milionów, czyli o ponad 2 miliony więcej niż pod koniec 2016 roku. Wśród nich 60% korzystała z aplikacji mobilnych zainstalowanych na swoim telefonie komórkowym. Pozostali korzystają z tradycyjnych form, logując się przez przeglądarki. Liczba użytkowników rośnie w ogromnym tempie. Telefony

są obecnie jednym z najbardziej pożądanych form łączności nie tylko w sferze kontaktów, ale też przy dokonywaniu operacji finansowych czy zarządzaniu kontem. Do obecnych trendów w dziedzinie płatności mobilnych zalicza się BLIK, czyli jednorazowy kod, składający się z 6 cyfr za pomocą którego można płacić w sklepach, stacjonarnych czy internetowym lub wypłacać pieniądze z bankomatu.

Tabela 1. Liczba klientów „mobile only"

Bank	IV kwartał 2017	III kwartał 2017	Zmiana pomiędzy kwartałami
PKO BP	685 513	576 073	109 440
ING Bank Śląski	413 525	349 571	63 954
mBank	338 103	292 504	45 599
BZ WBK	326 088	274 330	51 758
Bank Millennium	311 000	148 000	163 000
Eurobank	36 905	34 603	2 302
Orange Finanse*	32 160	32 160	bd.
Citi Handlowy*	31 876	31 876	bd.
Raiffeisen Polbank	29 287	34 419	–5 132
Credit Agricole	20 333	17 265	3 068
TMUB	17 211	20 214	–3 003
Plus Bank	12 413	9 806	2 607
BGŻ BNP Paribas*	10 811	10 811	bd.
Alior Bank	10 549	9 358	1 191
Razem:	**2 275 774**	**1 840 990**	**434 784**

Źródło: Raport PRNews.pl: Liczba klientów mobile only – IV kw. 2017; https://prnews.pl/raport-prnews-pl-liczba-klientow-mobile-only-iv-kw-2017-433554.

Bankowość mobilna wykształciła pojęcie „mobile only", które oznacza zarządzanie własnymi finansami jedynie za pomocą smartfona. Ostatni kwartał 2017 roku pokazał, iż 2,3 mln klientów banków, tylko i wyłącznie za pomocą smartfona obsługiwało swoje konto, nie korzystając w tym czasie z tradycyjnych form logowania. Dane te pochodzą z raportu PRNews.pl [https://prnews.pl/raport-prnews-pl-liczba-klientow-mobile-only-iv-kw-2017-433554], w którym uwzględniono dane 11 największych banków w Polsce. Z przedstawionych poniżej danych wynika, że występuje tu tendencja wzrostowa w większości wymienionych przypadków. Największą rzeszę odbiorców mobile only ma bank PKO BP oraz ING Bank Śląski.

Bankowość mobilna, dzięki swojemu zastosowaniu, jest równie ceniona przez banki, ze względu na to, iż jest to jeden z najkorzystniejszych pod względem finansowania sposób oddziaływania na klienta. Rozwój wiąże się ze zwiększaniem efektywności w działaniach banku, szybkości przeprowadzania

transakcji, a także większej pewności przy niższych kosztach, co w konsekwencji powoduje zwiększanie się liczby odbiorów tych usług. Powiązania systemów informatycznych na których oparta jest bankowość mobilna pozwalają na częściowe zastąpienie pracy osób fizycznych, a także zapobiegają skutkom pomyłek, oszustw czy błędów. Poprzez aplikacje banki mogą obserwować zaangażowanie klientów w korzystaniu z usług mobilnych. Dzięki temu mogą regulować wachlarz swoich usług, dopasowując je do potrzeb klientów, jak również wprowadzać nowe udogodnienia pozwalające na utrzymanie obecnych klientów i zdobywanie nowych.

2.1. ZAGROŻENIA ZWIĄZANE Z KORZYSTANIEM Z M-BANKINGU

W Polsce na 45 973 916 klientów banków, aż 33 385 252 w ramach swojego rachunku bankowego posiada dostęp do bankowości internetowej, a ściślej 9 111 876 użytkowników to osoby korzystające z bankowości mobilnej minimum raz w miesiącu (stan na koniec IV kwartału 2017 roku). Względem IV kwartału 2016 r. liczebność tej ostatniej grupy wzrosła o blisko 2 mln. Pośród nich ponad połowa, tj. 5 173 184, korzysta z aplikacji mobilnej banku na telefonie komórkowym [Raport prnews.pl Polska bankowość w liczbach – IV kw. 2017]. Nieustanny wzrost liczby użytkowników oraz rozwój technologii ma przełożenie na rosnące zagrożenia związane z użytkowaniem smartfona w celach dostępu do oferty, jaką oferuje bank. Należy zwrócić uwagę, iż przestępcy bardzo sprytnie wykorzystują fakt, że mogą prowadzić swoje działania z niemalże każdego miejsca na świecie z dostępem do Internetu i nie potrzebują fizycznego kontaktu ani z potencjalną ofiarą, ani nawet pracownikiem banku. Na początku 2017 roku NBP opublikowało wyniki badania [https://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/Polacy-na-temat-uslug-bankowych_2016.pdf], z którego jasno wynika, że zdecydowanie ponad połowa Polaków w wieku do 24 lat aktywnie korzysta z usług oferowanych przez banki na urządzeniach mobilnych. Pod tym względem Polacy plasują się w europejskiej czołówce. Pośród badanych blisko 91% wykonuje minimum jedną transakcję w miesiącu za pośrednictwem aplikacji mobilnej bądź serwisu internetowego www. Obecnie w bankowości mobilnej istnieje zdecydowanie większe ryzyko niepożądanego dostępu do konta niż w bankowości internetowej. Składa się na to kilka czynników. Ataki hakerskie są coraz częściej wymierzane w użytkowników telefonów komórkowych. Za pomocą wiadomości SMS lub e-mail przestępcy przesyłają oprogramowanie szpiegujące lub wirusy w trakcie korzystania z usług i poprzez nakładki systemowe przechwytują wrażliwe dane. Jednakże najczęściej to nie poszczególni właściciele smartfonów są atakowani, a stacje przekazujące sygnały operatorów sieci. Dane transmitowane przez przekaźniki zostają przechwytywa-

ne i wykorzystywane przez osoby do tego nieuprawnione. Problematyczna może być również sytuacja, w której telefon zostaje zgubiony, ale głównie skradziony. Zanim nastąpi blokada rachunku bankowego z poziomu serwisu internetowego czy przy wykorzystaniu infolinii nasze konto może zostać okradzione. W dłuższej perspektywie czasu można myśleć optymistycznie na temat poprawy stanu obecnego. Banki zacieśniają bowiem współpracę z przedsiębiorstwami informatycznymi oraz operatorami sieci komórkowych w celu poprawy bezpieczeństwa sektora bankowości mobilnej. Kluczową kwestią są jednakże niewystarczająco wysokie nakłady pieniężne przekazywane na tego typu działania. Oprócz spraw czysto technologicznych dużą rolę odgrywa sam konsument. Klienci banków często nie spodziewają się ataków hakerskich, a wręcz nie są do nich przygotowani. Niestety w dalszym ciągu banki nie prowadzą ukierunkowanych kampanii informacyjnych na temat bezpiecznego poruszania się w tej jakże popularnej formie dostępu do rachunku bankowego, czyli bankowości mobilnej.

2.2. PRZYKŁADOWE SCHEMATY DZIAŁANIA CYBERPRZESTĘPCÓW I SPOSOBY POSTĘPOWANIA

Coraz częściej hakerzy ukierunkowują swoje działania na ataki na aplikacje mobilne banków poprzez inne, słabo lub wcale niezabezpieczone aplikacje znajdujące się w urządzeniu. Pod koniec listopada 2017 w sklepie Google Play zostały zamieszczone dwie aplikacje „CryptoMonitor" oraz „StorySaver". Pierwsza z wymienionych miała informować o aktualnych kursach popularnych w ostatnim czasie krytowalut, natomiast druga służyła do pobierania i zapisywania równie modnych tzw. „Instastories" z aplikacji Instagram. W rzeczywistości posłużyły cyberprzestępcom do zeskanowania danych użytkowników aż 14 banków. Schemat działania polegał na tym, iż aplikacje te tworzyły łudząco podobne wersje serwisów logowania do systemu bankowości elektronicznej, a następnie wymuszały logowanie się poprzez wyświetlanie fikcyjnych komunikatów m.in. o zaplanowanej przerwie technicznej lub ofertą przygotowaną przez bank. Podczas próby uzyskania dostępu przez użytkownika przechwytywały loginy oraz hasła, a w późniejszej fazie nawet SMSy autoryzujące transakcje. Podczas listopadowego ataku zostali okradzeni klienci najliczniejszych aplikacji: Alior Mobile, BZWBK24 mobile, Getin Mobile, IKO, Moje ING mobile, Bank Millennium, mBank PL, BusinessPro Nest Bank, Bank Pekao, PekaoBiznes24, plusbank24, Mobile Bank Citi Handlowy. M-banking stwarza ogromne możliwości i udogodnienia, jednakże również generuje coraz to nowe niebezpieczeństwa.

W połowie stycznia 2018 na stronie internetowej mBanku został umieszczony komunikat o następującej treści: „Nowe cyberzagrożenie z wykorzystaniem przekierowania połączeń na inny numer telefonu" [dostęp: 15.01.2018].

Po raz kolejny łamacze kodów opracowali nowy sposób na wdarcie się na rachunki bankowe obcych osób. Tym razem posługiwali się głównie danymi zgromadzonymi z fałszywych ogłoszeń o pracę i wykorzystywali je w celu ustawienia przekierowania połączeń i SMSów swoich ofiar u operatora telefonii komórkowej na inne numery. Kolejnym krokiem było sparowanie nowych urządzeń z aplikacją mobilną dzięki zdobytym wcześniej informacjom oraz przekierowanych wiadomości. Ostatnim etapem była już tylko kradzież środków z kont.

W obu z przedstawionych przypadków cyberprzestępcy bazowali na niewiedzy konsumentów z zakresu stosowania zabezpieczeń ich urządzeń oraz łatwowierności przy przekazywaniu ich danych osobowych.

2.3. METODY OCHRONY I ZASADY BEZPIECZNEGO PORUSZANIA SIĘ W M-BANKINGU

Pojęcie bezpieczeństwa w bankowości elektronicznej, a szczególnie w bankowości mobilnej, należy rozpatrywać na dwóch poziomach – banku oraz klienta. Eksperci z zakresu zabezpieczeń współczesnych banków zwracają uwagę, że obecnie stosowane rozwiązania należą do możliwie jednych z najbardziej zaawansowanych. Środki ochrony można podzielić w następujący sposób [Gąsiorowski i Podsiedlik 2015: 220, 221]:

1. Prawne – w skład której wchodzą wszelkie unormowania prawne dotyczące ochrony danych przetwarzanych w bankowych systemach informatycznych.
2. Fizyczne – do której zaliczają się zabezpieczenia, funkcjonujące w otoczeniu systemu informacyjnego, a nie stanowiące jego części.
3. Techniczne – są to wszelkiego rodzaju rozwiązania sprzętowe związane z informatyką lub wykorzystujące technologie informatyczne i w sposób bezpośredni wpływające na bezpieczeństwo systemu.
4. Programowe – zaliczamy do tej kategorii wszelkie rozwiązania zabezpieczające, które dostępne są dzięki wykorzystywaniu oprogramowania zarówno systemowego, jak i aplikacyjnego.
5. Organizacyjne – które dotyczą kontroli zarządzania i procedur bezpieczeństwa.
6. Kryptograficzne – szyfrujące przesyłane informacje tak, aby jedynie jej odbiorca był w stanie odczytać wysłaną przez nadawcę wiadomość.

Komisja Nadzoru Finansowego przedstawia za pośrednictwem swojego portalu zbiór podstawowych zasad bezpieczeństwa w bankowości elektronicznej, a więc również mobilnej, wśród nich występują [Zasady bezpieczeństwa…, dostęp: 21.09.2015]:

1. Nie udostępniaj loginu i haseł do systemu bankowości elektronicznej.
2. Regularnie zmieniaj hasła do systemu bankowości elektronicznej.

Tabela 2. Biometria w bankach w Polsce (stan na 13.09.2017)

Biometria w bankach w Polsce (stan na 13.09.2017)	
Alior Bank	Logowanie odciskiem palca do aplikacji iOS. W planach wdrożenie dwóch kolejnych metod weryfikacji biometrycznej – biometrii głosu i biometrii twarzy.
BGŻ BNP	Bank korzysta z biometrii w kontekście podpisu elektronicznego w jednym z kanałów. Logowanie odciskiem palca powinno się pojawić w nowej aplikacji mobilnej.
BZ WBK	Logowanie odciskiem palca do aplikacji iOS. W planach system Android. System biometrii głosowej na infolinii. Trwają testy wideoweryfikacji.
Citi Handlowy	Logowanie odciskiem palca do aplikacji (Android i iOS).
Eurobank	Logowanie odciskiem palca do aplikacji (Android i iOS).
Getin Bank	Logowanie odciskiem palca do aplikacji Getin Mobile i Noble Mobile (Android i iOS).
ING Bank Śląski	Logowanie odciskiem palca do aplikacji (Android i iOS dla klientów detalicznych, iOS dla klientów korporacyjnych).
mBank	Logowanie odciskiem palca do aplikacji iOS.
Millennium	Logowanie odciskiem palca do aplikacji (Android i iOS). Możliwość potwierdzania odciskiem palca transakcji 3D Secure.
Pekao	Logowanie odciskiem palca dla klientów korporacyjnych korzystających z systemu bankowości internetowej PekaoBiznes24. W nowej aplikacji mobilnej będzie logowanie odciskiem palca.
PKO BP	Testy bio stanowisk umożliwiających weryfikację tożsamości osób z wykorzystaniem ich cech osobniczych takich jak podpis, skan naczyń krwionośnych dłoni, głos czy skan twarzy. Logowanie odciskiem palca do aplikacji (Android i iOS).
Plus Bank	W planach biometria w aplikacji mobilnej.
Raiffeisen Polbank	Od listopada 2017 logowanie poprzez Touch ID w Mobilnym Portfelu.

Źródło: https://www.bankier.pl/wiadomosc/Biometria-w-bankowosci-Co-za-jej-pomoca-zalatwimy-dzis-w-banku-7542743.html.

3. Nie otwieraj budzących wątpliwości linków w otrzymywanych wiadomościach SMS oraz e-mail.

4. Zainstaluj i aktualizuj oprogramowanie antywirusowe, zarówno na komputerze, jak i na urządzeniu mobilnym oraz aktualizuj na bieżąco system operacyjny urządzenia i jego aplikacje lub programy.

5. Regularnie sprawdzaj, czy numery rachunków bankowych do przelewów zdefiniowanych i cyklicznych nie uległy podmianie.

6. Przed wpisaniem kodu potwierdzającego wykonanie operacji sprawdzaj numery rachunków bankowych.

7. Przeglądaj cyklicznie historię rachunku i operacji z nim związanych, a w przypadku dostępności usługi powiadomień SMS o każdej wykonywanej operacji aktywuj ją.

8. Samodzielnie wpisuj numery rachunków bankowych bez stosowania funkcji „kopiuj–wklej".

9. Nie korzystaj z systemu bankowości za pośrednictwem niezabezpieczonych łącz internetowych, w tym hot-spotów w miejscach publicznych.

10. Używaj oprogramowania z legalnego i zaufanego źródła.

Konsumenci często zapominają, lub nawet wcale nie stosują niektórych z wyżej wymienionych czynności. Przekładanie wygody nad odpowiedzialnością jest zjawiskiem niemalże codziennym, a udogodnienia jakie oferują zaplanowane przelewy np. za ratę kredytu lub opłatę związaną z lekcjami kursu językowego lub kopiowania numeru rachunku bankowego ze strony konkretnej instytucji, bądź faktury elektronicznej stanowią doskonały punkt zaczepienia dla cyberprzestępców. Od kilku lat ta sytuacja poziomu zabezpieczeń ulega znacznej poprawie za sprawą rozwoju i wykorzystywaniu przez banki biometrii.

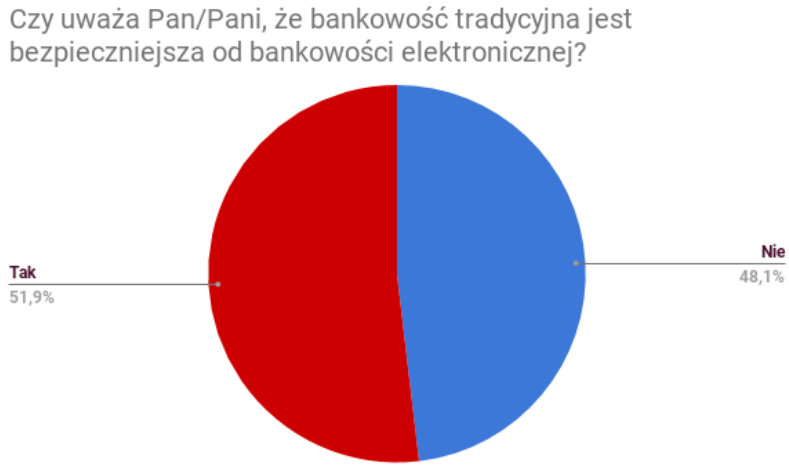
Tabela 2 prezentuje zastosowania przez system funkcji biometrycznych – odcisku linii papilarnych palca, biometrii twarzy, głosu oraz skanu naczyń krwionośnych dłoni.

3.1. POZIOM ŚWIADOMOŚCI KONSUMENTÓW WOBEC CYBERPRZESTĘPCZOŚCI W BANKOWOŚCI MOBILNEJ NA PRZYKŁADZIE STUDENTÓW LUBELSKICH UCZELNI

Badania przeprowadzone zostały na grupie 187 ankietowanych – byli to studenci lubelskich uczelni wyższych. Większość z nich studiuje kierunki ekonomiczne. W ankiecie padały pytania o preferencje korzystania z aplikacji mobilnych, poziom świadomości zagrożeń wynikających z tego typu udogodnień czy znajomość sposobów zabezpieczania. Na podstawie odpowiedzi ankietowanych można oszacować, na jakim poziomie lubelscy studenci są informowani przez banki, a także istnieje możliwość zidentyfikowania ich znajomości sfery bankowości mobilnej. Z przeprowadzonych badań wynika, iż 17,1% ankietowanych nie korzysta z bankowości mobilnej, zaś 82,9% jest w jej posiadaniu bądź używa jej w życiu codziennym.

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

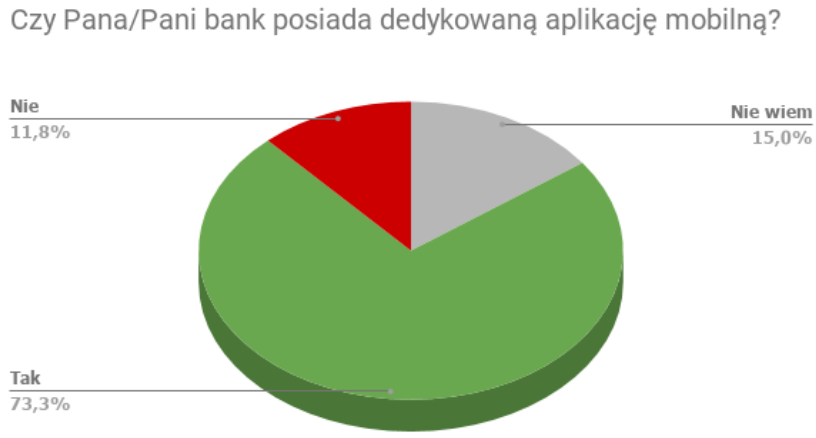
Jak można zauważyć najczęściej wykorzystywaną aplikacją służącą logowaniu sie do bankowości mobilnej jest Google Android.



Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Studenci są skłonni również twierdzić, iż bankowość tradycyjna jest jednak bardziej bezpieczną formą użytkowania i niesie za sobą mniej zagrożeń.

Ankietowani wśród zabezpieczeń najczęściej wymieniają: hasła SMS, hasła jednorazowe, PIN i obrazek bezpieczeństwa. Okazuje się, że większość korzysta z dokładnie tych samych form. Co ciekawe, duża liczba osób w celu dostępu do systemu bankowości nie korzysta z bezpłatnych hot-spotów WiFi (61%), co jest obecnie jednym z poważnych zagrożeń. Pozostali najczęściej wykorzystują hot--spoty w centrach handlowych, hotelach bądź uczelniach publicznych.



Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Odsetek ankietowanych, który nie jest pewien czy ich bank posiada dedykowaną aplikację mobilną, świadczy o tym, iż konsumenci są mało poinformowani przez banki w których posiadają rachunki o tego typu udogodnieniach. Większość korzysta z aplikacji na smartfonie, tylko nieliczni używają do tego tabletów, podobnie jest zaś ze stronami www.

Ciekawe okazuje się wykorzystanie form płatności. Najwięcej zwolenników mają przelewy na rachunek bankowy, BLIK czy przelew na numer telefonu. Zapomniane są takie formy jak: Android Pay czy NFC, HFC. Wynikać to może z niedostosowania możliwości oferowanych usług przez operatorów sieci, gdyż obecne smartfony bądź usługi które są udostępniane klientom, posiadają wymienione formy płatności. Z tego względu duży odsetek ankietowanych nawet nie wie o ich istnieniu, co przekłada się na negatywne wyniki ankiety.

Konsumenci usług bankowych, mimo wielu akcji, nie znają niebezpieczeństw wynikających z użytkowania bankowości mobilnej. Wyłudzanie danych, kradzieże spowodowane złym oprogramowaniem, sczytywanie danych z kart płatniczych czy kradzieże przy płatnościach internetowych przez powiązanie banku z obsługą aplikacji zakupowych, wiele osób nie wie czym są bądź

nigdy nie słyszało o zabezpieczeniach nakładanych przez banki. Nieliczna grupa potrafi wymienić wszystkie z nich. Poziom świadomości niestety nie jest zadowalający. Banki mimo prowadzonych kampanii czy korespondencji wysyłanej do klientów, nie są w stanie skutecznie poinformować klientów o wszystkim tym, co powinni wiedzieć. Być może nie chcą, aby ich nie odstraszać, zasypując ich coraz to nowymi informacjami.

3.2. CZYNNIKI RYZYKA ZWIĄZANE Z DZIAŁANIAMI UŻYTKOWNIKÓW

Należy wyraźnie zaznaczyć, iż użytkownicy, podobnie jak banki, są współodpowiedzialni za bezpieczeństwo zlecanych operacji. Już na etapie tworzenia dyspozycji przelewu, a nawet instalowania aplikacji mobilnej, od konsumenta zależy czy jego bezpośrednie działania są bezpieczne. Tylko posiadacz konta decyduje z jakiego urządzenia skorzysta i to w jego intencji jest upewnienie się że jest ono bezpieczne, czyli czy posiada stosowne oprogramowanie zabezpieczające. Również kwestia cyklicznej zmiany hasła zależy od zaangażowania użytkownika, bowiem może on dopisać do bieżącego hasła jeden znak lub stworzyć całkowicie inne, co jest jedynym słusznym rozwiązaniem. Współczesne tempo życia oraz natłok informacji docierających z różnych źródeł i niekiedy wzajemnie się wykluczających ma wpływ na niechęć konsumenta do edukacji na tematy technologii z jakiej korzystają. Dane zawarte w raporcie Związku Banków Polskich [https://zbp.pl/public/repozytorium/dla_bankow/raport_ZBP_ cyberbezpieczny_ portfel.pdf] obrazują poziom kluczowego czynnika w tym zakresie jakim jest wiedza. 10% respondentów wskazuje, że wiedza klientów banków na temat bezpieczeństwa kształtuje się na wysokim poziomie, niemalże 3/4 (72%) twierdzi, że poziom wiedzy jest jedynie przeciętny, kolejne 17% ocenia poziom jako niski, a 1% badanych nie ma zdania.

PODSUMOWANIE

Współcześnie bankowość mobilna cieszy się bardzo wysoką i nieprzerwalnie rosnącą popularnością. Stopniowo obserwujemy marginalizację bankowości tradycyjnej, gdyż jest ona wypiera przez szeroko pojętą bankowość elektroniczną. Ciągły postęp technologiczny ma odzwierciedlenie w liczbie użytkowników urządzeń mobilnych takich jak smartfon, tablet czy laptop. Generuje to w dużym stopniu rozwój m-bankingu oraz wymusza na bankach sprostanie oczekiwaniom ich klientów w zakresie oferowanych usług, ale też ich jakości. Szybkie tempo życia i informatyzacja przestrzeni publicznej jest również istot-

nym czynnikiem, który wpływa na chęć coraz sprawniejszego dostępu do usług finansowych.

W związku z powyższym rola placówek bankowych częściej przybiera formę oddziału doradczego w zakresie wykonywania czynności dostępnych za pośrednictwem systemu bankowości elektronicznej. Z pewnością w dalszym ciągu będą pełniły one istotne role w sektorze bankowym, zwłaszcza iż wiele klientów ma pewne obawy związane z wirtualną bankowością. Oczywiście nowe szanse płynące z postępu stwarzają kolejne zagrożenia, które wpływają na odbiorców usług. Zjawiskiem towarzyszącym obecnej sytuacji jest cyberprzestępczość, a natłok oferowanych informacji w postaci reklam, newsletterów itp., sprzyja jej wzrostowi. Głównym zagrożeniem dla konsumenta jest on sam. Nieuważne korzystanie z poczty elektronicznej czy nagminne korzystanie z publicznych sieci Wi-Fi typu hot-spot generuje niepotrzebne ryzyko przejęcia danych przez hakerów. W takich przypadkach nawet wydające się najlepsze zabezpieczenia biometryczne nie są w stanie skutecznie ochronić rachunku bankowego przed nieuprawnionym dostępem przez osoby trzecie.

Słowem podsumowania, bankowość mobilna jako szczególny typ bankowości elektronicznej posiada niezmierzony potencjał i stwarza ogromne ułatwienie w codziennym funkcjonowaniu klientom banków. Badania przeprowadzone na grupie studentów jednakże jasno ilustrują opisywany problem bezpieczeństwa, a także potwierdzają zasadność hipotezy, że obecny poziom wiedzy uniemożliwia w pełni bezpieczne korzystanie z innowacyjnych rozwiązań, jakie oferuje bankowość mobilna.

BIBLIOGRAFIA

Bolibok P., Bolibok A., 2014, *Bankowość mobilna jako innowacyjny kanał dostępu do usług bankowych*, „Roczniki Ekonomii i Zarządzania", nr 6(42).

Gąsiorowski J., Podsiedlik P., 2015, *Przestępstwa w Bankowości elektronicznej w Polsce*, Wydawnictwo Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza.

Guzek E., Ślązak E., 2012, *Innowacyjna bankowość internetowa: Bank Web 2.0*, Wydawnictwo Wolters Kluwer Polska, Warszawa.

https://www.bankier.pl/wiadomosc/Biometria-w-bankowosci-Co-za-jej-pomoca-zalatwimy-dzis-w-banku-7542743.html [dostęp: 2017.09.13].

https://prnews.pl/raport-prnews-pl-liczba-klientow-mobile-only-iv-kw-2017-433554 [dostęp: 27.02.2018].

Koćwin J., 2017, *Bankowość mobilna w Polsce – innowacje a bezpieczeństwo klientów*, [w:] E. Rutkowska-Tomaszewska (red.), *Ochrona klienta na rynku usług finansowych w świetle aktualnych problemów i regulacji prawnych*, C.H. Beck, Warszawa.

Koźliński T., 2017, Departament Systemu Płatniczego, opublikowano: styczeń 2017 r., https://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/Polacy-na-temat-uslug-bankowych_2016.pdf.

Niczyporuk P., Talecka A., 2011, *Bankowość. Podstawowe zagadnienia*, Wydawnictwo Temida 2, Białystok.
Niewiadomski K., Zakonnik Ł., 2017, *Bankowość mobilna w Polsce – przegląd aplikacji, ranking, możliwości rozwoju*, „Przedsiębiorczość i Zarządzanie", t. 18, z. 4, cz. 1.
Nowe cyberzagrożenie z wykorzystaniem przekierowania połączeń na inny numer telefonu, https://www.mbank.pl/informacje-dla-klienta/indywidualny/post,8094.html [dostęp: 15.01.2018].
Pearce J., 2013, *Programowanie mobilnych stron internetowych z wykorzystaniem systemów CMS*, Wydawnictwo Helion, Gliwice.
Raport #CYBERBEZPIECZNY PORTFEL – Zasady Bezpieczeństwa, opublikowano: grudzień 2016 r., https://zbp.pl/public/repozytorium/dla_bankow/raport_ZBP_cyberbezpieczny_portfel.pdf.
Ślązak E., 2017, *Kanały dystrybucji w bankach*, [w]: J. Koleśnik (red.), *Bankowość detaliczna*, Difin, Warszawa.
Zasady bezpieczeństwa w bankowości elektronicznej, https://www.knf.gov.pl/poprzednie_lata/komunikaty?articleId=53878&p_id=18 [dostęp: 21.09.2015].

NEW THREATS AND METHODS OF PROTECTION OF FINANCIAL SERVICES IN THE MOBILE BANKING SECTOR

Abstract

The purpose of this article is to examine consumer awareness in the use of mobile banking in Poland. The evolution of mobile banking as well as the scale of its occurrence are also presented. The study presents the results of a survey conducted in the form of a survey, the level of knowledge and typical habits when using m-banking for students of Lublin universities. In addition, examples of cybercriminals' methods of operation based on information presented by selected banks and financial sector institutions are discussed.

Keywords: mobile banking, virtual banking, mobile technologies, cybercrime.

Przyjęto/Accepted: 10.06.2018
Opublikowano/Published: 30.06.2018